Atty. Docket No.: 042390.P9257
Express Mail No.: EL466330405US

APPLICATION FOR UNITED STATES PATENT

FOR

CREATION AND DISTRIBUTION OF A SECRET VALUE BETWEEN TWO DEVICES

Inventor:

DAVID W. GRAWROCK

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(714) 557-3800

CREATION AND DISTRIBUTION OF A SECRET VALUE BETWEEN TWO DEVICES

BACKGROUND

1. FIELD

This invention relates to the field of data security. In particular, the invention relates to a platform and method for generating and distributing a secret value between multiple devices.

2. BACKGROUND

In electronic commerce, it is becoming necessary to transmit digital data from one location to another in a manner that is clear and unambiguous to a legitimate receiver, but incomprehensible to any illegitimate recipients. Accordingly, such data is typically encrypted by a software application executing some predetermined encryption algorithm and is transmitted to the legitimate receiver in encrypted form. The legitimate receiver then decrypts the transmitted data for use.

Often, encryption/decryption of data is accomplished through symmetric key cryptography. For symmetric key cryptography, the sender uses a secret value as a key to encrypt data prior to transmission over an unsecured link. The receiver uses the same secret value as a key to decrypt the data upon receipt. One problem associated with symmetric key cryptography is that it is difficult for devices, such as platforms or integrated circuit components for example, to distribute a secret value in a secure manner.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an exemplary embodiment of a platform practicing the invention.

Figure 2 is an exemplary embodiment of an integrated circuit (IC) component as a Trusted Platform Module (TPM) employed within the platform of Figure 1.

Figure 3 is an exemplary embodiment of the generation of a Long Term Value (LTV).

Figure 4 is a more detailed embodiment of the generation of a Long Term Value (LTV) between the TPM and ICH of the platform of Figure 1.

Figure 5 is an exemplary embodiment of the generation of a Short Term Value (STV).

Figure 6 is a more detailed embodiment of the generation of a Short Term Value (LTV) between the TPM and ICH of the platform of Figure 1.

Figure 7 is an exemplary embodiment of a block diagram for generation of a unique secret value for a communication session through the combination of the LTV and the STV internally within a device.

DESCRIPTION

The present invention relates to a platform and method for generating and distributing a secret value between multiple devices. The specific manner selected in generating the secret value can provide two advantages; namely, it can logically bind the devices together for subsequent verification that the devices are in close physical proximity to one another and mitigates replay attacks.

Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, certain terminology is used to discuss features of the present invention. For example, a "device" includes include one or more integrated circuit components or one or more products that process data such as a computer (e.g., desktop, laptop, server, workstation, personal digital assistant, etc.), a computer peripheral (e.g., printer, facsimile, modem, etc.), wireless communication device (e.g., telephone handset, pager, etc.), a television set-top box and the like. A "link" is broadly defined as a logical or physical communication path such as, for instance, electrical wire, optical fiber, cable, bus trace, or even a wireless channel using infrared, radio frequency (RF), or any other wireless signaling mechanism.

In addition, "information" is generally defined as one or more bits of data, address, control or any combination thereof. "Code" includes software or firmware that, when executed, performs certain functions. Examples of different types of code include an application, an applet, or any series of instructions. A "communication session" is a series of operations used to transfer information between two platforms in a secure manner. The session may terminate automatically when the transfer of information has completed, after a predetermined time has elapsed, or under control by any of the communication session participants.

I. General Platform Architecture

Referring to Figure 1, an exemplary block diagram of an illustrative embodiment of a platform 100 employing the present invention is shown. The platform 100 comprises a processor 110, a memory control hub (MCH) 120, a system memory 130, an input/output control hub (ICH) 140, and an integrated circuit (IC) component

150 which controls security of the platform 100. The components of platform 100 may be employed on any substrate (e.g., circuit board, removable card, etc.) or multiple substrates.

As shown in Figure 1, the processor 110 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or a hybrid architecture. In one embodiment, the processor 110 is compatible with the INTEL® Architecture (IA) processor, such as the IA-32 and the IA-64. Of course, in an alternative embodiment, the processor 110 may include multiple processing units coupled together over a common host bus 105.

Coupled to the processor 110 via the host bus 105, the MCH 120 may be integrated into a chipset that provides control and configuration of memory and input/output (I/O) devices such as the system memory 130 and the ICH 140. Typically, the system memory 130 stores system code and data. The system memory 130 is typically implemented with dynamic random access memory (DRAM) or static random access memory (SRAM).

The ICH 140 may also be integrated into a chipset together with or separate from the MCH 120 to perform I/O functions. As shown, the ICH 140 supports communications with the IC component 150 via link 160. Also, the ICH 140 supports communications with components coupled to other links such as a Peripheral Component Interconnect (PCI) bus at any selected frequency (e.g., 66 megahertz "MHz", 100 MHz, etc.), an Industry Standard Architecture (ISA) bus, a Universal Serial Bus (USB), a Firmware Hub bus, or any other bus configured with a different architecture other than those briefly mentioned.

Referring to Figure 2, an exemplary embodiment of the IC component 150 is shown as a Trusted Platform Module (TPM), which features one or more integrated circuits placed within a protective package 200. For instance, the protective package 200 may be any type of IC package such as an IC package for a single IC or a package for a multi-chip module. Alternatively, the protective package 200 may include a cartridge or casing covering a removable circuit board featuring the integrated circuit(s) and the like.

As shown in Figure 2, the TPM 150 comprises an I/O interface 210, a processor 220, internal memory 230, an asymmetric key generation unit 240, at least one cryptographic engine 250 and a random or pseudo random number generator 260

(generally referred to as a "number generator"). The number generator 260 may be employed within the asymmetric key generation unit 240 or operates in cooperation therewith.

Herein, the internal memory 230 includes one or more memory components, including at least non-volatile memory and perhaps volatile memory. Typically, these different memory types are employed as different components.

In general, the number generator 260 (or alternatively the asymmetric key generation unit 240) generates a "long-term value" (LTV) 270 and a "short-term value" (STV) 280. The LTV 270 is stored within the non-volatile memory of the internal memory 230 while the STV 280 can be stored in either a non-volatile or volatile memory. Collectively, these values produce a secret value (SV) that is used as a cryptographic key for transmission of data between the ICH 140 and TPM 150 over link 160 in an encrypted and/or decrypted format.

The cryptographic engine(s) 250 supports encryption/decryption, digital signing and hashing operations. Although the cryptographic engine(s) 250 is illustrated as logic separate from the processor 220, it is contemplated that it may employed as part of the processor 220.

II. LTV Generation

Referring now to Figure 3, an exemplary embodiment of a block diagram illustrating the generation of a long term value (LTV) 270 is shown. In this embodiment, generation of the LTV 270 occurs in response to an event such as an initial power-up sequence by a substrate or platform featuring two or more devices 300 and 310 that are attempting to establish at least one secure communication channel over link 320. This power-up sequence may be performed during assembly of the platform, most likely during power-up of certain communicative devices after installation on the substrate.

In general, at initial power-up, the first device 300 may issue a control signal 330 to the second device 310, which signals the second device 310 to internally generate the LTV 270. Thereafter, the LTV 270 is permanently stored in a protected memory location such as, for example, within internal, non-volatile memory of the second device 310. In addition, the second device 310 also transmits the LTV 270 to the first device 300 for internal storage as well. Both devices 300 and 310 are now configured to ensure that the LTV 270 cannot be reprogrammed at a later time.

More specifically, for an embodiment featuring components of platform 100 of Figure 1, the ICH 140 detects an initial event (e.g., first power-up sequence) and is in communication with the TPM 150. As shown in Figure 4, upon detecting the initial power-up sequence, the ICH 140 issues a special command 400, referred to herein as "GenerateLTV," to the TPM 150 over link 160.

In response to receiving the GenerateLTV command 400, the TPM 150 generates the LTV 270. This may be accomplished by taking the next 160 bits from the number generator 260 employed within the TPM 150 for example. The TPM 150 saves the LTV 270 in non-volatile memory of internal memory 230 and protects this information from any modification or observation.

After generating the LTV 270, the TPM 150 returns the LTV 270 to the ICH 140 over link 160 as a response to the GenerateLTV command. The ICH 140 takes the LTV 270 and stores this value in an internal, non-volatile memory 410 of the ICH 140. The contents of the non-volatile memory 410 are protected from modification or observation.

As briefly described above, the GenerateLTV command is a one-time only command. The ICH 140 may be configured to protect itself from ever issuing this command again. One method of accomplishing this protection is to have the command protected by a fuse (not shown). Once the operation has completed, the LTV installer would blow the fuse so that the command would never be executable again. This fuse operation must also occur in the TPM 150 for the same reason.

III. STV Generation

Referring to Figure 5, an exemplary embodiment of a block diagram illustrating the generation of a short term value (STV) is shown. Generation of the STV 280 occurs in response to a periodic event such as during initialization of the devices within the platform for example. The STV 280 is stored in volatile memory of both first and second devices and is lost when power is disrupted to any of the devices.

In general, during a power-up cycle of the substrate or platform, the first device 300 locates the second device 310 and requests generation of the STV 280 by issuing a control signal 340 over link 350. The second device 310 generates a short term value once per power cycle. The STV 280 may be generated by a number generator for each power cycle or initially generated by the number generator in response to the power cycle and subsequently incremented for each communication session. Thus, the STV

would operate as a rolling nonce. The STV 280 is provided to the first device 300 for subsequent, temporary storage.

More specifically, for an embodiment featuring components of platform 100 of Figure 1, the first device (e.g., ICH 140) issues a special command 420, referred to as a "GenerateSTV" command, to the second device (e.g., TPM 150) as shown in Figure 6. In response to receiving the GenerateSTV command 420, the TPM 150 generates the STV 280. This may be accomplished by taking the next 160 bits from the number generator 260 employed within the TPM 150 for example. In this embodiment, the TPM 150 stores the STV 280 in a portion of internal memory 230 that may be volatile (as shown) or even erasable, non-volatile memory.

Moreover, the TPM 150 returns the STV 280 to the ICH 140 over link 160 as a response to the GenerateSTV command. The ICH 140 takes the STV 280 and stores this value in volatile memory 430 of the ICH 140. Both the ICH 140 and 150 protect the GenerateSTV command from multiple executions by using a sticky bit to only allow one operation per power cycle.

IV. Secret Value Generation

Referring now to Figure 7, both the LTV 270 and STV 280 are stored in non-volatile memory of a device 500 (e.g., TPM/second device 150/310 set forth above) and protected from observation and manipulation. The LTV 270 and STV 280, when combined by logic 510, generate a secret value (SV) 520. The SV 520 may be used by both devices as a cryptographic key to establish at least one secure communication channel between the multiple devices. Since the STV 280 is different for each power cycle, the SV 520 is unique for each communication session. This operation of combining the LTV 270 and the STV 280 is performed within each of the devices and is never provided outside the device over the communication link.

The term "combined" (or any tense thereof) is generally defined as a bit manipulation of two values such as a one-way hashing operation which converts a sequence of bits into a unique value having a fixed bit length. Thus, the logic 510 that performs the combining operation may be the processor 220 or the cryptographic unit 250. Of course, logic 510 may be configured to be independent from the processor 220 and the cryptographic unit 250.

V. Additional Security Features

It is contemplated that a link interconnecting a first device (e.g., an ICH) and a second device (e.g., a TPM) may be configured to support special bus cycles. These special bus cycles provide the second device greater assurances that the first device transmitted a signal (e.g., Generate STV) instead of an unauthorized outside source. In essence, this provides assurances that the first and second devices were in close proximity during manufacture.

Another feature is to initiate a time limit for receipt of the STV in response to the GenerateSTV command. This may be accomplished by employing a counter or other timing mechanism within the first device and determining whether the STV is provided by the second device before a selected time or count has elapsed. By imposing a time constraint, it provides greater assurances that the devices are in close proximity.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art. Additionally, it is possible to implement the present invention or some of its features in hardware, firmware, software or a combination thereof where the software is provided in a processor readable storage medium such as a magnetic, optical, or semiconductor storage medium.